THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE

BRET TUCKER FANNING
individually and as the Surviving Spouse and Next of Kin of Shanda Fanning,

Plaintiff,

v.

Honeywell Aerospace, a division of Honeywell International, Inc., and Honeywell International Inc.

Defendants

Case No.: 3:14-cv-01650

Judge Haynes

MEMORANDUM OF LAW IN SUPPORT OF PLAINTIFF'S MOTION TO COMPEL HONEYWELL TO PRODUCE REQUIREMENTS DOCUMENTS AND SOURCE CODE FOR THE EGPWS MODEL AT ISSUE IN THIS CASE

At the heart of this case is the design of the software in the Honeywell Enhanced Ground Proximity Warning System ("EGPWS"). As the name suggests, the purpose of the EGPWS is to warn pilots when, for whatever reason, the aircraft is in immanent risk of crashing into the ground. On the early morning of August 14, 2013, as UPS Flight 1354 was approaching the Birmingham Alabama International Airport, the Honeywell EGPWS did not warn the pilots of the plane's proximity to the ground. Indeed, the Honeywell EGPWS did not issue a "terrain" warning until one second *after* the aircraft impacted terrain and crashed. Plaintiff's wife, Shanda Fanning, who was the First Officer (co-pilot) on the flight, was killed along with the Captain.

The Honeywell EGPWS uses the known height of the aircraft above the ground and its position compared to a terrain database to calculate where the aircraft is in relationship to terrain

and then uses computer software to determine when to issue a warning that the aircraft is too close to terrain. The answer to why the Honeywell EGPWS only issued a "terrain" warning one second after the plane impacted terrain is necessarily contained in the design of the EGPWS, its software, and particularly in the software's source code which determines when the EGPWS will issue a warning.

Plaintiff's burden in this product liability suit, generally, is to show that the Honeywell EGPWS failed to perform as it should have. To do that, Plaintiff must have full access to certain Honeywell documents and the source code. Those documents are the "System Requirements Document," ("SRD") and "Software Design Requirements Document" ("SDRD") (collectively "the Requirements Documents"). These documents establish *what* the Honeywell EGPWS and its software are required to do. The source code for the EGPWS is then designed to accomplish *how* the Honeywell EGPWS will meet those requirements. Notwithstanding the Plaintiff's need for this critical information, Honeywell has refused to produce the Requirements Documents under the existing negotiated and court-ordered Protective Order, and refuses to provide any access to the source code whatsoever.

Incredibly, as part of its basis for not providing these critical documents, Honeywell contends that Plaintiff hasn't, with sufficient particularity, identified exactly the claimed defect in the Honeywell EGPWS. While Plaintiff has more than satisfied its burden of showing these documents are relevant and discoverable, Honeywell's contention actually highlights how critical these documents and the source code are. The specificity that Honeywell claims Plaintiff must attain can only be obtained through the documents and source code Honeywell refuses to produce. Accordingly, Plaintiff brings the instant motion.

Honeywell has demanded that the Requirements Documents requested by Plaintiff only be produced for limited inspection subject to overly burdensome and unreasonable restrictions. Those restrictions include that only portions of the Requirements Documents can be selected by Plaintiff based on blind review of a table of contents; that those portions must be approved by Honeywell before they may be inspected by Plaintiff; that those documents can only be inspected in-person at Honeywell's facility in Redmond, Washington without any ability to even take notes; and that only then will those portions (not objected to by Honeywell) be produced, and only in an overly restrictive electronic format that cannot be practically used by Plaintiff's experts.

The Requirements Documents, which describe what the EGPWS should do – not how it should do it – are not remotely so sensitive that they necessitate the burdensome restrictions Honeywell seeks to impose. They can and should be produced subject to the terms of the protective order already entered in this case intended to cover precisely such documents.[1]

Honeywell's complete refusal to produce the software source code for the EGPWS is likewise improper. There can be no question that the software source code is relevant to Plaintiff's claims of design defect in the EGPWS. Plaintiff has alleged that multiple modes and functions of the EGPWS caused or contributed to the crash and should have been more safely designed. Review of the EGPWS software source code is the only way for Plaintiff's experts to determine specifically how the EGPWS at issue was defectively designed as well as demonstrate how a reasonable alternative design could have avoided the subject crash. While Plaintiff

[1] Indeed, Honeywell's attempts to have the Requirements Documents treated as more than merely confidential, is part of a pattern of over-designation that, for instance, seeks to have documents that are publicly available treated as "confidential." *See*, *infra*, p. 9, n.4.

acknowledges Honeywell's interest in protecting its source code, and is willing to abide by reasonable restrictions, Honeywell's denial of any access whatsoever is meritless. Access to software source code is routinely granted by courts. Indeed, Honeywell has previously produced the software source code for its EGPWS in legal proceedings when it was in its own interest as part of litigation against a direct competitor. Accordingly, Honeywell should be compelled to produce its source code, subject to the reasonable restrictions set forth in Plaintiff's Proposed Protective Order attached hereto.

I. Applicable Legal Standard

Under Federal Rule of Civil Procedure 26(b)(1), "[p]arties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit." Rule 26(c)(1)(G) also allows a party seeking to avoid discovery of relevant information to seek a protective order requiring that "a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only a specified way."

"It is within the sound discretion of the trial court to decide whether trade secrets are relevant and whether the need outweighs the harm of disclosure. Likewise, if the trade secrets are deemed relevant and necessary, the appropriate safeguards that should attend their disclosure by means of a protective order are also a matter within the trial court's discretion." *R.C. Olmstead, Inc., v. CU*

Interface, LLC, 606 F.3d 262, 269 (6th Cir. 2010) (quoting *Centurion Indus., Inc. v. Warren Steurer & Assocs.*, 665 F.2d 323, 326 (10th Cir.1981)).

In this case, the court has already entered an Agreed Protective Order on March 10, 2015, which was negotiated and agreed to between the parties in precise contemplation of "trade secret or other confidential research, development, or commercial information" being produced in discovery. (Copy attached hereto as Ex. A, ¶ 2.1). As a result, the vehicle for protecting "confidential" or "trade secret" information already exists. Importantly, unlike the vast majority of cases involving discovery of trade secret information, "this is not a case where a competitor is the party seeking the information, . . . where courts may be more willing to grant protective orders because of the certainty that the information would in fact be obtained by the competitor and the obvious likelihood of competitive injury." *Waelde v. Merck, Sharp & Dohme*, 94 F.R.D. 27, 29 (E.D. Mich. 1981). Plaintiff is a widower – not a competitor of Honeywell – who seeks redress for the death of his wife – not to litigate a commercial dispute. The risk of harm to Honeywell is minimal and, indeed, nulled by virtue of the existing Agreed Protective Order.

II. Honeywell Should be Ordered to Produce the EGPWS Requirements Documents

A. Requirements Documents

What software engineers refer to as "system requirements documents" set forth the specifications of ***what*** the system must be able to do. (Affidavit of Glenn Haskins ("Haskins Aff."), attached hereto as Ex. B, ¶ 6). The system requirements document is then used to create what software engineers call the "high-level software requirements document," which sets forth the specifications of ***what*** the software must do to meet the system requirements. (*Id.*). From those documents, software engineers then create a detailed design document which sets forth ***how*** the

software will meet the specifications and accomplish the tasks set forth in the requirements documents. (*Id.*). All of these documents collectively are referred to as the "Requirements Documents". [2]

To use an analogy, if the EGPWS system was akin to a car, the system requirements document might set forth the requirement that the car must be able to reach zero to 60 miles per hour in six seconds. (*Id.*, at ¶ 7). The software requirements document would then set forth that the car will use an six-cylinder engine to accomplish the goal of going zero to 60 miles per hour in six seconds. (*Id.*). The detailed design document would then describe how the actual engine would be designed so that it would both have six cylinders and be able to go zero to 60 miles per hour in six seconds. (*Id.*).

B. Plaintiff's Requests for EGPWS Requirements Documents

Plaintiff's First Request for Production, served December 4, 2014, included request 16 seeking "[a]ll software specifications, including but not limited to all software requirements specifications and/or all software development specifications, for the 'Subject Model EGPWS'...." (attached hereto as Ex. C, p. 7).

In response, Honeywell objected that "software requirements specifications" and "software development specifications were" vague and overbroad, but agreed to produce responsive documents upon entry of a protective order by the Court. (Honeywell's Response to Plaintiff's First Requests for Production, attached hereto as Ex. D, p. 8-9).

[2] Honeywell's counsel has represented that the only documents responsive to Plaintiff's requests for documents relating to "software requirements specifications" are the SRD and SDRD. To the extent any other documents include the information that would normally be found in Requirements Documents, those documents would also be responsive to Plaintiff's requests and are covered by this motion.

During multiple "meet and confer" conferences between counsel, the parties crafted an agreed protective order and Plaintiff's counsel clarified that the terms "software requirements specifications" and "software development specifications," as used in the requests, were meant to include the Requirements Documents.

With the benefit of reviewing the documents produced by Honeywell in response to his First Request for Production (albeit not including the actual Requirements Documents) Plaintiff made even more specific requests for the Requirements Documents, naming them specifically by Honeywell document number in Plaintiff's Second Request for Production, served June 26, 2015 (attached hereto as Ex. E). Plaintiff's Second Request for Production included request 14 seeking the "System Requirements Document (SRD) for the Enhanced Ground Proximity Warning Computer, Honeywell document number 993-0976-303, revision New -01 (as referenced at HW003405)" and request 15 seeking the "Software Design Requirements Document (SDRD) for the Enhanced Ground Proximity Warning Computer, Honeywell document number 995-0104-610 (as referenced a HW003405)." (*Id.* at p. 8). In response, Honeywell now objected that the documents sought contained "trade secrets," but it was willing to meet and confer again. (Honeywell's Response to Plaintiff's Second Request for Production, attached hereto as Ex. F, p. 10-11).

On August 18, 2015, counsel for Plaintiff and Honeywell "met and conferred" regarding these discovery requests, and counsel for Honeywell stated that it would consult its client and consider whether it would be willing to produce the Requirements Documents. On October 8, 2015, Honeywell informed Plaintiff that it would only produce the requested Requirements Documents for the EGPWS if Plaintiff agreed to a proposed draft Second Protective Order with

additional onerous restrictions beyond those provided in the Agreed Protective Order already entered in the case. (Copy attached hereto as Ex. G).

C. The Relevance and Necessity of Production of the Requirements Documents Outweighs the Risks to Honeywell Under the Existing Protective Order

To date, plaintiff's investigation, based in part on the NTSB investigation into this case, has identified EGPWS Modes 1 and 2B, as well as the EGPWS's Forward Looking Terrain Avoidance ("FLTA") and Terrain Clearance Floor ("TCF") enhanced functions, as design features of the Honeywell EGPWS that are at issue in this suit.[3] These features, it is alleged, should have provided the pilot with alerts that would have notified him to avoid terrain thus forming the basis of Plaintiff's product liability case. By not producing this critical information about these features Honeywell is essentially thwarting Plaintiff's ability to carry his burden of proving the specific design feature that was defective, *Nemir v. Mitsubishi Motors Corp.*, 381 F.3d 540, 550-51 (6th Cir. 2004) (denying defendant's motion for a protective order in a products liability suit because granting the order would deprive plaintiff's attorney from being able to prepare his case through reasonable access to relevant information), including by showing how a reasonable alternative design could have made the product safer and avoided this crash. *See, e.g., Martin v. Michelin N. Am., Inc.*, 92 F. Supp. 2d 745, 754 (E.D. Tenn. 2000).

1. Relevance and Necessity of Mode 1 Requirements Information

Mode 1 of the EGPWS provides alerts to pilots for excessive descent rates by comparing the aircraft's descent rate to its altitude above the ground. (Mk V and VII EGPWS Pilot's Guide, copy attached hereto as Ex. H, HW000014). When the descent rate is excessive considering the

[3] For a description of what each feature is supposed to do and why it is relevant, see discussion, *infra*, p. 8-14.

aircraft's proximity to the ground, a "Sinkrate" warning should be issued by the EGPWS. Based on the parameters set forth in the EGPWS Product Specification, it appears that a Mode 1 "Sinkrate" caution alert should have been issued much earlier than actually took place during the flight at issue. According to the specifications provided by Honeywell, the subject aircraft met the qualification for a "Sinkrate" alert when it was at 294 feet altitude. (EGPWS Product Specification, attached hereto as Ex. I, HW003202, HW003246-49; [4] NTSB Systems Group Chairman's Factual Report ("Systems Group Report"), attached hereto as Ex. N, p. 6-7). However, the EGPWS did not issue a "Sinkrate" caution alert until the aircraft was at 195.8 feet altitude (Systems Group Report, Ex. J, p. 7). The NTSB determined that a difference of only approximately 40 feet (or approximately 3-4 seconds) could have allowed the captain to avoid the terrain of the subject flight (*see* NTSB Aircraft Performance Group Chairman's Study Report ("Aircraft Performance Study"), Ex. K, p. 27, 71). Why the Mode 1 feature did not perform as advertised should be determinable from the Requirements Documents and/or Source Code.[5]

Moreover, the conditions for when a "Sinkrate" alert should be issued existed for at least 5 seconds (Systems Group Report, Ex. J, p. 8), but the flight data recorder ("black box") indicates that the "Sinkrate" alert was only activated for three seconds. (Flight Data Recorder Group Chairman's Factual Report, attached hereto as Ex. L, p. 10-19). While the Product

[4] Notably, Honeywell designated the subject model EGPWS Produce Specification as "confidential" even though the Product Specification for a similar EGPWS is publicly available on its website. (EGPWS MK VI and VIII Product Specification available at https://www51.honeywell.com/aero/common/documents/Mk_VI_ VIII_ EGPWS,P-Ns_965-1176-XXX.pdf)

[5] The NTSB seemingly accepted Honeywell's explanation based upon the way the data was recorded – rather than the EGPWS performance – at face value without further investigation, let alone after review of the Requirements Documents and/or Source Code. (*See* Ex. I, HW012772.)

Specification for the EGPWS references that there is "filtering"[6] of the radio altitude signal used for Mode 1, it is not described in any meaningful way in the material produced by Honeywell to date. (Ex. I, HW003238, HW003248-49). That information, however, should certainly be present in the Requirements Documents and if so would provide critical insight into how and why the EGPWS performed – or failed to perform – as it did.

In addition, Honeywell indicates that the Mode 1 "Sinkrate" caution should issue multiple times based on a "time to impact" equation, which it set forth in an email to the NTSB investigators. (Email from Honeywell to NTSB, attached hereto as Ex. M, HW012774-76). Applying this equation to the flight data, it appears that the EGPWS should have issued multiple "Sinkrate" alerts in this case. (*Id.*, at HW012775). Multiple "Sinkrate" alerts, however, were *not* issued on the subject flight before it crashed. The "time to impact" equation does not appear in the EGPWS Product Specification and Plaintiff, therefore, cannot determine exactly how it functions or how it would have impacted the issuance of alerts in this case. That information should, however, be available in the Requirements Documents and would provide critical insight into how and when the EGPWS performed or failed to perform as it did.[7]

In order to fully understand the function of EGPWS Mode 1, determine precisely how the design is defective, and identify how an alternative design could have been implemented, Plaintiff needs the more detailed information about Mode 1 that is found in the Requirements Documents.

---

[6] A software "filter" is software code that examines input data (in this case radio altitude data that determines the "Sinkrate") and only allows certain data that meets particular criteria to be considered.

[7] Plaintiff has requested documents relating to any "filters" applied to data used for Mode 1 and how the "time to impact" calculation works (Plaintiff's 2nd Requests for Production, Ex. E, requests 4 through 12, 39 through 41, 45 through 47). Honeywell has represented that the only additional responsive documents that could provide the information Plaintiff is seeking are the

2. Relevance and Necessity of Mode 2B Requirements Information

EGPWS Mode 2 "provides alerts to help protect the aircraft from impacting the ground when rapidly rising terrain with respect to the aircraft is detected" by comparing the aircraft's radio altitude (measured by radio waves from an on-board radar pointed at the ground) to the rate at which that radio altitude is decreasing and issuing a "Pull Up" warning to the pilot. (Mk V and VII EGPWS Pilot's Guide, copy attached hereto as Ex. H, HW000015). Mode 2B is active when the aircraft's flaps are in the landing configuration or the aircraft is making a localizer approach, as this aircraft was at the time of the crash. (*Id.*, at HW000018).

Based on the parameters for Mode 2B (EGPWS Product Specification, Ex. I, HW003203-04, HW003250, HW003253-54), and the altitude and descent rate information set forth in the NTSB's Aircraft Performance Study, there should have been a Mode 2B "pull up" alert issued in this instance, but was not. (Email from NTSB to Honeywell dated March 5, 2011, attached hereto as Ex. N, HW006422). In explaining why there was no Mode 2B "pull up" alert in this case, Honeywell informed the NTSB that the recorded radio altitude data is passed through multiple limiters and filters. (Email from Honeywell to the NTSB dated , attached hereto as Ex. O, HW009067-68).[8]

None of the documents produced by Honeywell to date describe the limiters and filters applied by the EGPWS in Mode 2B in the detail that would allow Plaintiff to properly assess whether EGPWS Mode 2B was negligently or defectively designed. Honeywell has indicated that the only additional responsive documents that could provide the information Plaintiff is

---

SRD and SDRD.

[8] The NTSB apparently accepted Honeywell's explanation at face value without examining what limiters and filters were used; why they were used; and whether a better design could have been

seeking are the EGPWS Requirements Documents. As a result, the Requirements Documents are necessary to Plaintiff's ability to prove his negligent design and design defect claims.

3. Relevance and Necessity of TCF Requirements Information

The EGPWS's Terrain Clearance Floor ("TCF") function is designed to alert the pilot of descent below a defined height above the underlying terrain, which is dependent on the distance from the nearest runway, based on the aircraft's radio altitude. (Pilot's Guide, Ex. H, HW000032). While the EGPWS did issue a TCF "terrain" alert in this case, it did so only *after* the aircraft had already impacted terrain. (Systems Group Report, Ex. J, p. 9).

The Terrain Clearance Floor levels surrounding each runway depend on what is called the envelope bias factor, which Honeywell states is based on "position accuracy". (Product Specification, Ex. I, HW003270-71). There is also indication, based on the NTSB's investigation that there is a one second persistence requirement for TCF alerts, which is not set forth in the documents Honeywell has presented to date. (Systems Group Report, Ex. J, p. 9). In addition, the radio altimeter information that the TCF function relies upon to issue alerts is also apparently subject to some kind of limiting or filtering that prevents excessive descent rates from being registered from the radio altimeter and prevents TCF alerts from being issued. (Product Specification, Ex. I, HW003238).

None of the documents produced by Honeywell to date, however, describe the filters or limits on radio altimeter data used by the TCF function, or describe in detail how "position accuracy" is determined. While Plaintiff has requested additional documents relating to all of these features of the TCF function (Plaintiff's 2nd Requests for production, Ex. E, requests 4

---

accomplished.

through 12), Honeywell has indicated that the only additional responsive documents that could provide the information Plaintiff seeks are the Requirements Documents.

4. Relevance and Necessity of FLTA Requirements Information

The Honeywell EGPWS has a Forward Looking Terrain Avoidance ("FLTA") function that looks ahead along the aircraft's flight path to "detect terrain or obstacle conflicts with greater alerting time." (Honeywell's Pilot's Guide, Ex. H, HW000035). The FLTA system uses "sophisticated algorithms" that compare "aircraft position, flight path angle, track, and speed relative to the terrain database image forward [of] the aircraft" to generate alerts regarding terrain ahead of the aircraft on its current flight path. (*Id.*).

The EGPWS is supposed to be designed to issue alerts that will provide the pilot with ample warning to allow him or her to undertake the necessary action to avoid colliding with an obstacle or terrain. Here the aircraft was descending into rising terrain ahead of it on a flight path angle that would unavoidably lead to impact with that terrain. Yet an alert was not issued until *after* terrain was impacted. As the NTSB found, with the appropriate warning, a successful climb maneuver could have been accomplished with as little as approximately 40 additional feet (or approximately 3-4 seconds) warning. (NTSB Aircraft Performance Study, Ex. K, p. 27, 46, 71).

What remains unclear is why no FLTA warning was issued *at all* before the aircraft impacted terrain. None of the documents produced by Honeywell to date adequately address this issue. While Plaintiff has requested additional documents relating to the FLTA and the 400-foot cutoff (Plaintiff's 2nd Requests for Production, Ex. E, requests 4 through 12, and 57 through 59; Plaintiff's 4th Requests for Production, attached hereto as Ex. Q, requests 14 through 18),

Honeywell has indicated that the only additional responsive documents that could provide the information Plaintiff seeks are the Requirements Documents.

Information relating to EGPWS Modes 1 and 2, as well as the FLTA and TCF functions – the features that should have provided alerts to the pilot that would have allowed the pilot to avoid this crash but did not – go to the heart of Plaintiff's claim that the EGPWS was defectively designed. The critical information necessary to properly and fully assess the design of these features can only be obtained, as Honeywell admits, from the Requirements Documents. These documents are not only highly relevant but necessary for Plaintiff to prove his case against Honeywell.

D. The Draft Second Protective Order Demanded by Honeywell Places Excessive Restrictions on Production that are Needlessly Expensive and Inefficient

Honeywell has refused to produce the Requirements Documents sought by Plaintiff, under the negotiated Agreed Protective Order. Instead Honeywell now demands that it only produce the EGPWS Requirements Documents subject to an even more onerous "Proposed Second Protective Order," and through burdensome and unreasonable processes. (Ex. G). The Requirements Documents, which only speak to *what* the EGPWS is supposed to do – not *how* – are covered by the existing protective order, which already covers "trade secret information". The proposed Second Protective Order would put a number of completely unnecessary, and arguably harassing, hurdles and restrictions upon Plaintiff that would thwart the way his experts can analyze and assess the EGPWS and, thereafter thwart Plaintiff's ability to prepare his case.

Under its Proposed Second Protective Order, Honeywell would, first, *only* produce the tables of contents of the Requirements Documents. Plaintiff's counsel would then have to blindly – without knowing what is in those portions of the Requirements Documents – identify which portions it wished to review and, incredibly, do so with a "good faith description" of how the requested

portions are relevant to his case. (*Id.*, at ¶ 5.1). There is no reasonable justification, let alone any basis in the Rules of Civil Procedure for such an unfair and prejudiced limiting of the scope of discovery, particularly given that there is already an Agreed Protective Order in place that covers those documents.

Honeywell's proposal would then go on to give Honeywell 15 days in which to bring a motion to prevent Plaintiff's counsel from even viewing any of those portions to which Honeywell objected. (*Id.* ¶ 5.2(1)). If Honeywell did not object to producing any portions of the Requirements Documents sought by Plaintiff, it would then only produce the portions of the Requirements Documents for visual inspection in a secured room at its facility in Redmond, Washington, across the country from both Plaintiff's counsel and this Court. (*Id.* at ¶ 5.2(2)). Plaintiff's counsel would then still have to identify, from those limited portions, the precise sections they wished to have copied, outlining in writing again how those portions are relevant and cannot be obtained from other sources. (*Id.* at ¶ 5.3). At that point, Honeywell would yet again have the opportunity to object to production of copies of the portions of the Requirements Documents to Plaintiff's counsel. (*Id.* at ¶ 5.3). Finally, if all of these hurdles are overcome, and Honeywell agrees to produce the portions of the Requirements Documents it deems in its own opinion are relevant (or is ordered to produce them by a court), those portions would only be produced in a highly restrictive document format with all copy and print functions disabled (*Id.* at ¶ 6), which prevents Plaintiff's counsel and his experts from properly reviewing them, or from even using the Requirements Documents as part of expert reports, court filings and as exhibits.

Honeywell is attempting to impose a level of discovery protection upon the Requirements Documents that are reserved only for the most sensitive trade secrets. While the Requirements

Documents may be confidential commercial information, they are not nearly as sensitive as, for instance, source code. The existing Agreed Protective Order more than adequately provides the protections to which Honeywell is entitled.

Honeywell's anticipated argument that the local Washington State FAA office reviews the requested Requirements Documents under similar conditions *for certification purposes* is a red herring. There is no doubt that the FAA has the authority to request any Honeywell documentation, including even source code, to review when and where it sees fit. *See* 14 C.F.R. § 21.610.[9] Simply because the local FAA office, might choose to review documents at Honeywell's facilities for certification purposes, does not mean at all that these are reasonable restrictions for purposes of inspecting and analyzing such documents in a civil product liability suit pending in Tennessee.

Further, Honeywell has previously produced Requirements Documents in litigation, including to competitors. In *Honeywell Int'l, Inc. v. Universal Avionics Sys. Corp.*, Honeywell produced Requirements Documents, like the ones sought by Plaintiff in this case, to its competitors Universal Aviation and Sundstrand who Honeywell had sued to enforce its EGPWS patents. 343 F. Supp. 2d 272, 288-89 (D. Del. 2004) aff'd, 488 F.3d 982 (Fed. Cir. 2007). Honeywell should not be allowed to demand such onerous restrictions upon Plaintiff concerning the Requirements Documents in this wrongful death lawsuit, when it freely provided them to potential customers and competitors to further its own business interests.

The Proposed Second Protective Order also seeks to give Honeywell improper control over Plaintiff's experts beyond what is reasonably necessary to protect its trade secrets. Under

[9] 14 C.F.R. § 21.610 requires that holders of certified equipment like Honeywell "allow the FAA to inspect its quality system, facilities, technical data, and any manufactured articles and witness any tests, including any inspections or tests at a supplier facility, necessary to determine

Honeywell's Proposed Second Protective Order, the only people authorized to access the information in the Requirements Documents are certain expert witnesses who Honeywell has approved based on presentation of expert's current and past employment and consulting information . (Proposed Second Protective Order, Ex. G, ¶ 4(c)). If Honeywell determines that "any identified individual is currently employed, consulting for or contracted by a competitor of Honeywell's EGPWS business *or otherwise represents a potential concern to Honeywell's trade secrets*" it could object and file a motion to prevent Plaintiff's counsel from giving that expert access to the Requirements Documents. (*Id.*) (emphasis added).

However, "the use of experts is virtually essential to the trier of the facts in examining and evaluating the structural parts of a computer program[,]" *Dynamic Microprocessor Associates v. EKD Computer Sales*, 919 F. Supp. 101, 105 (E.D.N.Y. 1996) (internal citations omitted) (citing *Computer Associates Intern., Inc. v. Altai, Inc.*, 982 F.2d 693, 714–15 (2nd Cir. 1992)). This is particularly the case with respect to the EGPWS system involved in this case. This is a very complicated and unique product, and it is difficult, if not impossible, to find an expert in EGPWS technology that has not also worked for a Honeywell competitor, including working on a competing product. In situations where a party requires a very specific expertise relating to the subject of the litigation, courts have found that it is permissible for that party to retain an expert, even one affiliated with a competitor, to receive confidential materials relating to the product at issue. *RR Donnelley & Sons Co. v. Xerox Corp.*, No. 12 C 6198, 2013 WL 6696652, at *2-3 (N.D. Ill. Dec. 19, 2013) (allowing disclosure of confidential and attorney's eyes only materials to an expert who had worked as a consultant for multiple competitors of the producing party because "the number of

---

compliance" with its regulations.

experts in the relevant field are small" and plaintiff's need for an expert outweighed defendant's concerns given the limits set by the protective order) (opinion attached hereto as Ex. R). Plaintiff should, likewise, not be so constrained here, particularly given the safeguards of the existing protective order, which prevents disclosure of confidential information by experts, and adequately protects any interest Honeywell may have in this regard.

This court should compel Honeywell to produce the EGPWS Requirements Documents sought by Plaintiff subject to the existing Agreed Protective Order entered in this case.

III. Honeywell Should be Ordered to Produce the Relevant Portions of the EGPWS Software Source Code Subject to Plaintiff Proposed Protective Order

A. Software Source Code

Computer programs, such as that found in the Honeywell EGPWS, are made up of lines of text written in computer coding language called "source code". (Affidavit of Glenn Haskins, Ex. B, ¶ 12); *SAS Inst. Inc. v. World Programming Ltd.*, 64 F. Supp. 3d 755, 761-62 (E.D.N.C. 2014). Computers themselves, however, can only read digital machine code made up of ones and zeros. (Haskins Aff., Ex. B, ¶ 12); *SAS Inst. Inc.*, 64 F. Supp. 3d at 761-62. A separate program called a compiler is used to translate source code from the programming language in which it was written to machine code in ones and zeros that can be read by a computer. (Haskins Aff., Ex. B, ¶ 13); *SAS Inst. Inc.*, 64 F. Supp. 3d at 761-62. Therefore to properly evaluate the EGPWS, including to evaluate whether certain "bugs" exist in the software or to evaluate alternative designs, one must have the source code and the compiler used by the EGPWS so that it can be run it on a computer and thoroughly evaluated. (Haskins Aff., Ex. B, ¶ 13).

B. Plaintiff's Requests for EGPWS Software Source Code

Request 29 of Plaintiff's First Request for Production sought "[t]he software code for the software that was installed on the 'Subject EGPWS' at the time of the 'Subject Crash'." (Ex. C, p. 8). In response, Honeywell objected that the request was overly broad and sought trade secret information. (Ex. D, p. 14).

After Honeywell's counsel refused to produce source code during multiple "meet and confers," Plaintiff served his Second Request for Production, which included request 13 seeking "the following source code files as referenced in the Software Accomplishment Summary for the EGPWC (at HW00386) for the Subject Model EGPWS: . . . f. Software Source Media, EGPW Application Software, Honeywell document number 996-011S-4X:X". (Ex. E, p. 7-8).

Honeywell responded to request 13 of Plaintiff's Second Request for Production as follows: "Honeywell objects to this request as it seeks trade secret or other confidential research, development, proprietary or commercial information from Honeywell and as currently drafted, seeks documents that are neither relevant to the present action nor reasonably calculated to lead to the discovery of admissible evidence." (Ex. F, p. 9). During multiple subsequent "meet and confers" Honeywell repeatedly refused to produce the source code under any circumstances.

C. The Relevance and Necessity of Producing the EGPWS Source Code Outweighs Any Risk to Honeywell Given the Safeguards that Will be in Place

There can be no serious dispute that the EGPWS software source code is highly relevant to the core issues in this case. In order to prove a design defect in the source code, as alleged, Plaintiff must have access to that part of the design of the EGPWS so it can be analyzed by experts and explained to the court and the jury through expert testimony. A common and persuasive way of proving a design defect is by showing there was a reasonable alternative design that could have practically been adopted at the time the product was sold. *See Martin*, 92 F. Supp. 2d at 753-54.

Here, that would entail showing how the EGPWS source code was designed, and how it could have been designed so as to provide an earlier warning to the pilot.

As addressed above, Plaintiff has identified EGPWS Modes 1 and 2B, as well as the FLTA and PDA functions, whose design caused or contributed to the subject crash. These modes are all critically dependent upon, and indeed defined by, the source code that implements them. Without access to the source code, Plaintiff would lack adequate information to determine the specific defects in the design of those modes that caused or contributed to the subject crash. Not only would the source code relating to those modes and functions be critical in allowing Plaintiff to determine the precise design defects at issue but, more importantly, it is the only reasonable way for Plaintiff to establish that there was a reasonable alternative design available using just "tweaks" to the available source code. *See In re Toyota Motor Corp. Unintended Acceleration Mktg., Sales Practices, & Products Liab. Litig.*, 978 F. Supp. 2d 1053, 1088 (C.D. Cal. 2013) (holding that determination of software design expert who had reviewed source code was relevant and admissible). Plaintiff's expert Glenn Haskins believes that changes in the EGPWS source code would likely provide a reasonable alternative design that would have allowed the EGPWS to warn the flight crew of in time to avoid this crash. (Haskins Aff., Ex. B, ¶ 14).

Furthermore, there is ample precedent for production of source code, even though it is a trade secret, in cases where it is relevant, including cases alleging design defect such as this one. *See, e.g.*, *R.C. Olmstead, Inc., v. CU Interface, LLC*, 606 F.3d 262, 267 (6th Cir. 2010) (ordering production of source code in copyright suit); *Burd v. Ford Motor Co.*, No. 3:13-CV-20976, 2015 WL 3705679, at *8 (S.D.W. Va. June 12, 2015) (ordering production of source code in order to allow plaintiffs to examine the code for defects in order to prove their products liability and negligent design claims)

(Ex. S); *Rensselaer Polytechnic Inst. v. Apple Inc.*, No. 1:13-CV-0633 DEP, 2014 WL 1871866, at *5, *6 (N.D.N.Y. May 8, 2014) (ordering defendant in software patent suit to produce all existing source code relating to the subject of the lawsuit) (Ex. T); *Dynamic Microprocessor Associates v. EKD Computer Sales*, 919 F. Supp. 101, 106 (E.D.N.Y. 1996) (ordering production of software source code in software copyright suit to enable defendant to determine whether it had indeed made an unauthorized copy of plaintiff's software); *Ameranth, Inc. v. Pizza Hut, Inc.*, No. 11-CV-1810-JLS-NLS, 2013 WL 636936, at *4 (S.D. Cal. Feb. 20, 2013) (ordering production of portions software source code relevant to plaintiff's claims in software patent suit) (Ex. V).

Indeed, Honeywell has previously produced EGPWS software source code in *Honeywell Int'l, Inc. v. Universal Avionics Sys. Corp.*, when it was seeking to enforce its patents. *See* 343 F. Supp. 2d 272, 283-84, 286 (D. Del. 2004) aff'd, 488 F.3d 982 (Fed. Cir. 2007). In that case, Honeywell sued two different manufacturers of competing products for violation of its EGPWS patents, and produced its EGPWS software source code information to prove its case. *Id.* But when it comes to a products liability suit against it, Honeywell claims that the confidential trade secret nature of its source code precludes production. Honeywell should not be allowed to use the source code was a sword and a shield.

D. Plaintiff's Attached Proposed Protective Order Provides Reasonable Safeguards for the Production of the EGPWS Software Source Code

Unlike the Requirements Documents discussed above, which only describe the specifications that the EGPWS software must meet, the source code for the EGPWS software embodies how the EGPWS works to accomplish the items set forth in the Requirements Documents and as such is a "trade secret". As such, Plaintiff recognizes that the EGPWS software source code may deserve stricter protection than is provided by the Agreed Protective Order already in place.

Plaintiff's proposed Source Code Protective Order provides for an encrypted copy of the source code in its original form, along with any compilers necessary to run the code be provided to Plaintiff's designated expert(s). (Source Code Protective Order, attached hereto as Ex. V, at ¶¶ 4(c), 6(a)-(f), (i)). Plaintiff's expert(s) with access to the source code will not be employed or consulting for a company that manufactures a competing product to Honeywell's EGPWS. (*Id.*, at ¶ 4(c)). Plaintiff's designated expert(s) will be the only one(s) allowed to open and run the source code on a computer that is not connected to the internet and is located within a locked room to which only he or she will have access. (*Id.*, at ¶¶ 6(l), (m)). Even within that room, the source code, as well as any files containing analysis of that code, will not be stored on the computer itself, but on a hard disk that shall be disconnected and placed in a locked container in the secured room when not in use. (*Id.*, at ¶ 6(k), (o), (p)).

While some courts have ordered production of source code only on a stand-alone computer in a secure location, sometimes at the producing party's facility, this is unduly burdensome to the requesting party and does not allow for fair access that is needed for proper evaluation of the source code. Such an approach is based on a faulty understanding of what truly keeps source code secure. Software encryption – rather than simply physical access –is what keeps source code secure. *See* Lydia Pallas Loren and Andy Johnson Laird, *Computer Software-Related Litigation: Discovery and the Overly-Protective Order*, 6 FED. CTS. L. REV. 5, 11 (2012) (attached hereto as Ex. W, at 35). All that is accomplished by limiting access to a stand-alone computer located anywhere other than the software expert's office is an increase in the time, cost and effort of examination of the source code. (*Id.*). Plaintiff's counsel and experts would need to travel to a remote location just to conduct their review which itself would be limited in terms of hours of access, ability to properly study the

source code, and would limit, if not preclude, their ability to take notes, with the Defendant's experts literally looking over the shoulder of Plaintiff's expert. Lastly, Plaintiff's expert(s) would not be able to run the source code to evaluate the EGPWS, or any modifications of the source code, to evaluate alternative designs.

Plaintiff's proposed protocol, while providing the requisite trade secret protection, does not unnecessarily restrict copying or printing of source code. Due to the unwieldy length of source code, software experts need to take notes, print and/or copy source code. However, they will only be permitted to print the most relevant and important portions of the source code that is necessary for them to carry out their purpose of examining the code and determining any flaws in its design. (*See id.*, at 43-44) (applying similar logic to review of source code to determine similarity in patent cases).

In sum, Plaintiff's Proposed Protective Order reasonably balances the need to allow Plaintiff's experts to review the source code efficiently and effectively, while also providing adequate protection for Honeywell's trade secret information.

V. Conclusion

In light of the foregoing, this court should order Honeywell to produce the EGPWS Requirements Documents under the existing protective order entered in this case, enter Plaintiff's Proposed Protective Order relating to production of software source code, and order Honeywell to produce the EGPWS software source code pursuant to that order.

Dated: New York, New York
January 15, 2016

KREINDLER & KREINDLER, LLP

/s/ *Daniel O. Rose*
Daniel O. Rose

Evan Katin-Borland
Admitted Pro Hac Vice
750 Third Avenue
New York, NY 10017
(212) 687-8181 - phone
(212) 972-9432 - fax
drose@kreindler.com
ekatinborland@kreindler.com

-and-

LANNOM & WILLIAMS, PLLC
B. Keith Williams, #16339
James R. Stocks, #25850
137 Public Square
Lebanon, TN 37087
(615) 444-2900 - phone
(615) 444-6516 - fax
keithwilliams@lannomwilliams.com
jimstocks@lannomwilliams.com

Attorneys for Plaintiff